UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/814,608	03/30/2004	Antonio Lain	B-5407 621797-2	5425

7590 05/07/2008

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
05/07/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/814,608	LAIN ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *March 30, 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 March 2004* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. 10/814,608.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/30/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the original filing of March 30, 2004. Claims (1-21) are pending and have been considered below.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-5, 8-17, 20 and 21 are rejected under 35 U.S.C. 102(b) as being anticipated by Chung Kei Wong (NPL "Secure Group Communications Using Key Graphs" and Wong hereinafter).

3. As to claim 1, Wong teaches a **apparatus for consolidating key updates provided in records** (i.e. message) **that each comprise an encrypted key** (e.g., group key) **corresponding to a node of a key hierarchy** and encrypted using a key (e.g., individual key) **which is a descendant** (i.e., root) **of that node** (i.e., Wong teaches a new key (k) with a one-to-one correspondence with a set of k-nodes. Wong teaches (K) contains a group key and individual key. Wong teaches the individual key is used to encrypt the group key [sec. I, pg. 17, par, 1, lines 1-5], [sec. II, pg. 18, par. A, "Key Graphs", line item 2]. Wong further teaches a key at the root of the tree shared by every user (e.g., group key) [sec II, pg. 18, par. B, "Special Classes of Key Graph", lines 13-16]) , **hierarchy-node information for both the encrypted and encrypting keys**

[sec. II, pg. 19, Table 1, "Number of Keys Held by the Server and Each User"], **and key-version information for at least the encrypted key** [sec. II, pg. 19, Table 1, "Number of Keys Held by the Server and Each User"];

the apparatus comprising a communications interface for receiving said records (i.e., set of User), **and a manager** (i.e., trusted key server) **for maintaining** (i.e., responsible for generating and distributing), **on the basis of the received records** (i.e., set of User), **a key tree** (i.e., key graph) **with nodes corresponding to nodes in said hierarchy, the manager** (i.e., trusted key server) **being arranged to store in association with each tree node** (i.e., Wong teaches a key graph with tow types of nodes [sec. II, pg. 18, par. A, "Key Graph", lines 1-6], **for each encrypting key** (i.e., individual key) **used in respect of the encrypted key** (i.e., group key) **associated with the node** (i.e., Wong teaches a new key (k) with a one-to-one correspondence with a set of k-nodes. Wong teaches (K) contains a group key and individual key. Wong teaches the individual key is used to encrypt the group key [sec. I, pg. 17, par, 1, lines 1-5], [sec. II, pg. 18, par. A, "Key Graphs", line item 2], **the most up-to-date version of the encrypted key and its version information** [i.e., sec. II, pg. 19, Table 1, "Number of Keys Held by the Server and Each User"] **with any earlier versions being discarded** (i.e., Wong teaches when a user leaves the server updates the key graph by deleting the user node and k node [sec. II, pg. 19, par. B, "Leaving a Star Key Graph"]).

4. As to claim 2, Wong teaches a **apparatus where the manager** (i.e., trusted key server) **is arranged to store** [i.e., sec. II, pg. 19, Table 1, "Number of Keys Held by the Server and Each User"] **each said most up-to-date version of a said encrypted key**

by storing the record containing the latter with any previously-stored record (i.e., u-node and k-node of leaving user) **that is thereby superseded being discarded** (e.g., delete). (i.e., Wong teaches server update key graph by deleting the u-node for the user and k-node for the individual key [sec. III, pg. 21, par. D, "Leaving a Tree key Graph", lines 1-3]).

5. As to claim 3, Wong teaches a **apparatus where the manager** (i.e., server) **is arranged to store in association with each tree node**, along with the most up-to-date version of the corresponding encrypted key stored for each encrypting key used in respect of that encrypted key, version information for the encrypting key used to encrypt said most up-to-date version of the encrypted key, **this version information being included in the record** (i.e., rekey message) **providing said most up-to-date version** (i.e., new group key) **of the encrypted key** (i.e., Wong teaches the server has to update the group's key graph by replacing the key s of some exiting k-nodes, deleting some k-nodes and adding some key nodes [sec. III, pg. 19, par. 2, lines 1-9]. Wong further teaches a rekey message distributed containing new group key).

6. As to claim 4, Wong teaches a **apparatus where the manager** (i.e., server) **is arranged to replace the version of the encrypted key stored in association with a tree node** (i.e., k-nodes) **for a particular encrypting key** (i.e., Wong teaches the server has to update the group's key graph by replacing the keys of some exiting k-nodes, deleting some k-nodes and adding some key nodes [sec. III, pg. 19, par. 2, lines 1-9]), **with any subsequently received later version of that key provided the latter**

has been encrypted with a version of the encrypting key that is the same or later than the version used for encrypting the existing stored encrypted key (i.e., Wong further teaches encrypting the newly generated group key with a the individual key of each remaining user [sec. III, pg. 19, par. B, "Leaving a Star Key Graph", lines 1-6]).

7. As to claim 5, Wong teaches a **apparatus further comprising a working-set generator for processing the key tree to generate** (e.g., create) **a subset** (i.e., new u-node and k-node) **of the tree enabling, at least within a target failure rate, all clients, associated with the key hierarchy to recover** (i.e., decrypt rekey message) **the current root key** (i.e., new group key) **of the latter** (i.e., Wong teaches a creating a new u-node, k-node and new group key for a new user join. Wong teaches distributing the new group key to existing user. Wong further teaches a rekey message containing the new group key sent to existing user, for which existing user decrypts it with the appropriate key in order to get the new one [sec. III, pg. 20, par. C, "Joining a Tree Key Graph" lines 1-18]).

8. As to claim 8, Wong teaches a **apparatus where the manager** (i.e., trusted key server) **is arranged to maintain said tree only in respect of keys corresponding to the nodes of a predetermined sub-hierarchy of said hierarchy and keys for the path from the head of this sub-hierarchy that terminates at the root of the hierarchy** (i.e., Wong teaches an approach of a hierarchy of keys, organized as a root tree [fig. 1]).

9. As to claim 9, Wong teaches a **system comprising apparatus and a key-hierarchy manager** (i.e., trusted key server) **for managing said key hierarchy in dependence on the addition and/or removal** (i.e., User Join/Leave) **of members to a group** (i.e., Wong teaches a trusted server responsible for group access control and key management [sec. **I**, pg. 17, par. A, "Our Approach", lines 13-16]), **the key-hierarchy manager** (i.e., trusted key server) **being arranged to output said records both to currently available members of said group and to said apparatus as notification of the changes made by the key-hierarchy manager to the key hierarchy** (i.e., Wong teaches sending a rekey message to user [sec. III, pg. 20, par. C, "Joining a Tree Key Graph", lines 13-18]), **said apparatus being arranged to provide said key tree** [fig. 1], **or a subset of it** [fig. 1], **to members of said group who subsequently become available as a consolidated notification of the changes made by the key-hierarchy manager** (i.e., trusted key server) **to the key hierarchy whereby to enable these members to recover the current root key** (i.e. Rekeying Strategies) **of the key hierarchy at least within a target failure margin** (i.e., Wong teaches rekeying strategies for new root key recovery [sec III]).

10. As to claim 10, Wong teaches **a system comprising apparatus and a key-hierarchy manager** (i.e., trusted key server) **for managing said key hierarchy in dependence on the addition and/or removal** (i.e., User Join/Leave) **of members to a group** (i.e., Wong teaches a trusted server responsible for group access control and key management [sec. **I**, pg. 17, par. A, "Our Approach", lines 13-16]), **the key-hierarchy manager being arranged to output said records to said apparatus** (i.e.,

Wong teaches sending a rekey message to user [sec. **III**, pg. 20, par. C, "Joining a Tree Key Graph", lines 13-18]), **said apparatus being arranged to provide said key tree** [fig. 1], **or a subset of it** [fig. 1], **to members of said group as a consolidated notification of the changes made by the key-hierarchy manager** (i.e., trusted key server) **to the key hierarchy whereby to enable these members to recover** (i.e. Rekeying Strategies) **the current root key of the key hierarchy at least within a target failure margin** (i.e., Wong teaches rekeying strategies for new root key recovery [sec III]).

11. As to claim 11, Wong teaches a **system where the key-hierarchy manager** (i.e., trusted key server) **and said apparatus form part of an anonymous group content distribution arrangement**; **the key tree** [fig. 1], **or a subset of it** [fig. 1], **being sent to group members in association with content encrypted with a key that is one of**:

- **the key-hierarchy root key** (i.e., individual key) [sec. **I**, pg. 17, par. 1, lines 1-5]),

- **a key** (i.e., group key) **encrypted using the key-hierarchy root key** (i.e., individual key) **and provided in encrypted form along with the encrypted content** (i.e., rekey message) (i.e., Wong teaches encrypting a group key with a individual key [sec. I, pg. 17, par. 1, lines 1-5]).

12. As to claim 12, Wong teaches a **system comprising multiple apparatuses and a key-hierarchy manager** (i.e., trusted key server) **for managing said key hierarchy**

in dependence on the addition and/or removal (i.e., User Join/Leave) **of members to a group and for outputting key update records** (i.e., sending rekey message) **reflecting changes made to the key hierarchy** (i.e., Wong teaches sending a rekey message to user [sec. III, pg. 20, par. C, "Joining a Tree Key Graph", lines 13-18]);

the apparatuses being configured in a multiple-level hierarchical arrangement [fig. 1] **comprising a first-level apparatus arranged to receive the records output by the key-hierarchy manager** [fig. 4 and fig. 5]**, and one or more lower levels of apparatuses each arranged to receive the key tree** [fig. 1]**, or a subset of it** [fig. 1]**, produced by a said apparatus at the next level up, the apparatuses at the lowest level of the hierarchical arrangement each being arranged to provide its key tree** [fig. 1]**, or a subset of it, to a respective sub-group of members of said group;**

the apparatuses at each level of said hierarchical arrangement [fig. 4]**, other than said first level, each being arranged to maintain its said tree only in respect of keys** (i.e., group keys) **corresponding to the nodes of a respective predetermined sub-hierarchy of said key hierarchy and keys for the path from the head of this sub-hierarchy that terminates at the root of the key hierarchy** (i.e., Wong teaches an approach of a hierarchy of keys, organized as a root tree [fig. 1]).

13. As to claim 13, Wong teaches a **method of consolidating key updates provided in records** (i.e., updating key graph base on Joins/Leaves) **each comprising an encrypted key** (i.e., group keys) **corresponding to a node of a key hierarchy and encrypted using a key** (i.e., individual key) **which is a descendant of that node** (i.e.,

Wong teaches encrypting a group key with a individual key [sec. I, pg. 17, par. 1, lines 1-5]), **hierarchy-node information for both the encrypted and encrypting keys, and key-version information for at least the encrypted key** [i.e., sec. II, pg. 19, Table 1, "Number of Keys Held by the Server and Each User"];

the method comprising a step of maintaining, on the basis of said records, a key tree with nodes (i.e., key graph/fig. 1) **corresponding to nodes in said hierarchy, this tree-maintenance step comprising a sub-step of storing in association with each tree node** (i.e., Wong teaches a trusted server responsible of key management [sec. I, pg. 11, par. A, "Our Approach", lines 14-24]), **for each encrypting key** (i.e., individual key) **used in respect of the encrypted key** (i.e., group key) **associated with the node, the most up-to-date version of the encrypted key and its version information with any earlier versions being discarded** (e.g., delete). (i.e., Wong teaches server update key graph by deleting the u-node for the user and k-node for the individual key [sec. III, pg. 21, par. D, "Leaving a Tree key Graph", lines 1-3]).

14. As to claim 14, Wong teaches a **method where in said sub-step each said most up-to-date version** (i.e., Table 1, "Number of keys held by the server and each user) **of a said encrypted key is stored by storing the record containing the latter with any previously-stored record** (i.e., u-node and k-node of leaving user) **that is thereby superseded being discarded** (i.e., Wong teaches server update key graph by deleting the u-node for the user and k-node for the individual key [sec. III, pg. 21, par. D, "Leaving a Tree key Graph", lines 1-3]).

15. As to claim 15, Wong teaches a **method where in said sub-step the version information of the encrypting key** (i.e., individual key) **used to encrypt said most up-to-date version of the encrypted key** (i.e., group key) **is stored with the latter** (i.e., Wong teaches server update key graph by deleting the u-node for the user and k-node for the individual key [sec. III, pg. 21, par. D, "Leaving a Tree key Graph", lines 1-3]). .

16. As to claim 16, Wong teaches a **method where in said sub-step the version of the encrypted key** (i.e., group key) **stored in association with a tree node for a particular encrypting key** (i.e., individual key)**, is replaced with any subsequently received later version of that key provided the latter has been encrypted with a version of the encrypting key that is the same or later than the version used for encrypting the existing stored encrypted key** (i.e., Wong teaches the server has to update the group's key graph by replacing the keys of some exiting k-nodes, deleting some k-nodes and adding some key nodes [sec. III, pg. 19, par. 2, lines 1-9]).

17. As to claim 17, Wong teaches **a method further comprising the further step of processing the key tree** (i.e., key graph/fig. 1) **to generate** (e.g., create) **a subset** (i.e., new u-node and k-node) **of the tree enabling, at least within a target failure rate, all clients associated with the key hierarchy to recover** (i.e., decrypt rekey message) **the current root key** (i.e., new group key) **of the hierarchy** (i.e., Wong teaches a creating a new u-node, k-node and new group key for a new user join. Wong

teaches distributing the new group key to existing user. Wong further teaches a rekey message containing the new group key sent to existing user, for which existing user decrypts it with the appropriate key in order to get the new one [sec. III, pg. 20, par. C, "Joining a Tree Key Graph" lines 1-18]).

18. As to claim 20, Wong teaches a **method where said tree is maintained only in respect of keys corresponding to the nodes of a predetermined sub-hierarchy of said key hierarchy and keys for the path from the head of this sub-hierarchy that terminates at the root of the hierarchy** (i.e., Wong teaches an approach of a hierarchy of keys, organized as a root tree [fig. 1]).

19. As to claim 21, Wong teaches a **method of providing key updates to members of a group, comprising the steps of:**

managing a key hierarchy (i.e., key graph/fig. 1) **in dependence on the addition and/or removal** (i.e., User Join/Leave) **of members to said group and outputting, as notification** (i.e., rekey message) **of the changes made to the key hierarchy** (i.e., key graph/fig. 1), **records that each comprise an encrypted key** (i.e., group key) **corresponding to a node of the key hierarchy and encrypted using a key** (i.e., individual key) **which is a descendant of that node** (i.e., Wong teaches encrypting a group with a individual key [sec. I, pg. 17, par. 1, lines 1-5]), **and hierarchy-node and key-version information for both the encrypted and encrypting keys version** (i.e., Table 1, "Number of keys held by the server and each user);

and consolidating said records (i.e., updating key graph base on Joins/Leaves) **according to the method and providing said key tree** (i.e., key graph/fig. 1), **or a subset of it** (i.e., key graph/fig. 1), **to members of said group whereby to enable these members to recover** (i.e., rekey strategies) **the current root key** (i.e., new group key) **of the key hierarchy at least within a target failure margin** (i.e., Wong teaches rekeying strategies for new root key recovery [sec III]).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

20. Claim 6, 7, 18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wong in view of Li (US Patent No. 6,606,706).

37. As to claims 6 and 18, the system disclosed by Wong discloses substantial features of the claimed invention. However, Wong fails to disclose;

> **A apparatus where the working set generator comprises control means for receiving feedback on the current root-key recovery failure rate and for controlling the size of said subset to approach the actual failure rate to said target failure rate** (claim 6).

> **A method where the further step comprises receiving feedback on the current root-key recovery failure rate and controlling the size of said subset to approach the actual failure rate to said target failure rate** (claim 18).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Wong as introduced by Li. Li discloses:

> **A apparatus where the working set generator comprises control means for receiving feedback on the current root-key recovery failure rate and for controlling the size of said subset to approach the actual failure rate to said target failure rate** (claim 6) (to provide the capability to receive rekey feedback from clients such that success/failure detection can be determine [col. 10, lines 55-67; col. 11, 1-10]).

A method where the further step comprises receiving feedback on the current root-key recovery failure rate and controlling the size of said subset to approach the actual failure rate to said target failure rate (claim 18) (to provide the capability to receive rekey feedback from clients such that success/failure detection can be determine [col. 10, lines 55-67; col. 11, 1-10]).

Therefore, given the teachings of Li, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Wong by employing the well known feature of client rekey feedback as disclosed above by Li, for which encryption key rekeying will be enhanced [col. 10, lines 55-67; col. 11, 1-10].

21. As to claim 7, Wong teaches a apparatus **where the working set generator further comprises means for determining the likelihood of a tree node being required to enable recovery the current root key, these means being based on at least one of the age of the node** (i.e., user-oriented rekey)**, or of an encrypted key associated with it** (i.e., Key-oriented rekey) **, and an estimate** (fig. 5) **of the number of possible clients that will need the node** (i.e., Wong teaches three approaches to construct rekey messages. Wong teaches rekeying approach constructs a rekey message that contains precisely the new keys needed by the user based on new user or existing user (i.e., **user age**) [sec **III**, pg. 20, par. 1, "User-Oriented Rekeying", lines 19-29]. Wong teaches each new key is encrypted individually for which each k-node

whose key has been changed the server will construct two rekey messages [sec III, pg. 20, par. 2, "Key-Oriented Rekeying", lines 1-13]).

22. As to claim 19, Wong teaches a **method where said further step further comprises determining the likelihood of a tree node being required to enable recovery the current root key** (i.e., rekey strategies), **this determination being based on at least one of the age of the node** (i.e. user- oriented rekey strategy), **or of an encrypted key associated with it** (i.e., key-oriented rekey strategy), **and an estimate of the number of possible clients that will need the node**.

Prior art made of record

23. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Medivsky (US Patent Publication No. 2004/0114762) Subset Difference Method for Multi-Cast Rekeying.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/

Examiner, Art Unit 2131

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2131